Digital Rights Management (DRM)

ISA 767, Secure Electronic Commerce
Xinwen Zhang, xzhang6@gmu.edu
George Mason University

Reference

- *Digital Rights Management: Business and Technology. New York: Hungry Minds/John Wiley & Sons, 2001.*

An example

- Buy a book in bookstore:
  - you get the right to read the book for as long and as many times as you want, and you can give, sell, or lend it to someone.
  - you can't legally make copies of it, change it, or embed parts of it in other works.

Changing of DRM

- New Technologies changes the rights management:
  - Digital format, easy to copy and manipulate
  - Internet-based distribution, cheap and instantaneous
  - New mechanisms for payment
- New business models:
  - dynamic pricing
  - permission to view content in exchange for user info (e.g., demographics)
  - syndicating content to other web sites
  - Other value-added service
- DRM: controlling and managing rights digital objects
  - Mostly IP objects

DRM Origin: Business Perspectives

- Super-distribution by Mori, 1983.
  - Consumer's further Distribution to other consumers
  - Digital objects are freely available to public in protected manner and only authorized users are allowed to use the objects
  - Can increase revenues by providing an opportunity to experience digital objects
- DRM first appeared in mid 90s for controlling distribution of consumer media

DRM Enforcement Tech

1. Legally, through registration forms, license agreements, and copyright laws.
2. Legally with an audit trail, such as copyright notices or watermarks (identifiers embedded permanently in the content).
3. Technologically, using encryption and user authentication to protect content and only make it accessible under strictly specified conditions.

DRM Origin: Technology Perspectives (1)

- As part of access control discipline
  - Since the advent of timesharing system (70's)
    - Multi-user OS
    - Need to share computing resource and information resource
  - Shift from mainframe to client-server and P2P
    - Needs to control digital objects even after distributions
  - Originator control policy in open environment
    - Originator's control at the outside of system

DRM Origin: Technology Perspectives (2) – by Rosenblatt et al.

- Software distribution
  - Availability of cheap Floppy disks, CD-RWs, DVD-RWs
  - Needs Protection schemes to prevent illegal copies
    - Warning message, product ID, activation, dongles
  - Software license admin in LAN
- Encrypted content distribution
  - Simple encryption scheme: Password, zip, etc.
  - Type fonts. Fonts are used to be expensive
  - Encrypt files on CD-ROMs

DRM Origin: Commercial History (1) – by Rosenblatt et al.

- Early commercial systems (beginning in 1994)
  - IBM infoMarket
    - All software-based
    - Cryptolope and a set of software for web-based marketplaces
  - Electronic Publishing Resources (EPR) later named as InterTrust
    - Originally an entire end-to-end system with hardware-based devices (including client-side hardware devices)
    - Later developed software-based systems
    - Now patent-based licensing, DRM interoperability

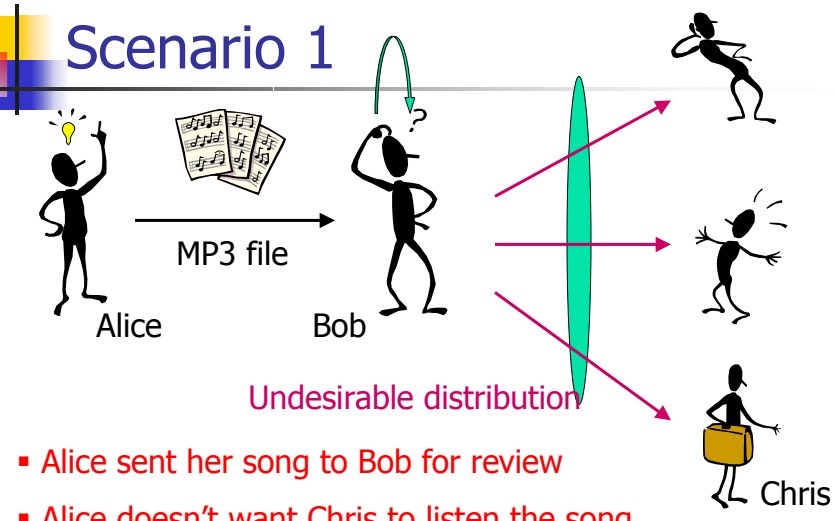
DRM Origin: Commercial History (2) – by Rosenblatt et al.

- Xerox PARC research labs
  - A new paradigm of DRM and Trusted Systems discussed in "letting loose the light" by Mark Stefik
    - in essence, it should always be possible to strictly define and control who can do what to a piece of content, when, on what devices, and for how much money or other form of consideration.
    - Based on *trusted system*
  - Digital Property Rights Language (DPRL) by Mark Stefik

DRM Origin: Commercial History (2) – by Rosenblatt et al.

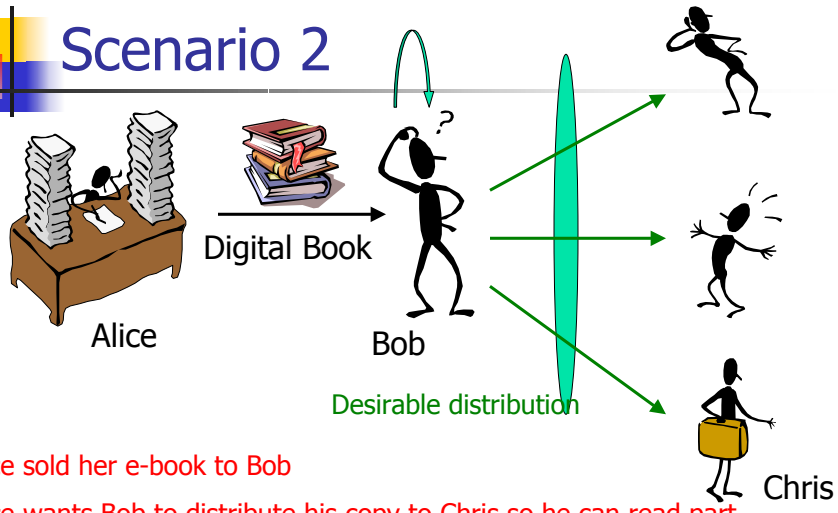
- ContentGuard's XrML
- Trusted Computing
  - Smart card, music player, etc
  - Intel LaGrande, TCG's NGSCB
- Watermarking Technologies
  - DigiMarc, …..

Scenario 1



- Alice sent her song to Bob for review
- Alice doesn't want Chris to listen the song

Scenario 2



- Alice sold her e-book to Bob
- Alice wants Bob to distribute his copy to Chris so he can read part of the book and become a potential customer (super-distribution)

Problems

- Unauthorized distribution & Use
  - Reproduction of a digital object does not reduce its quality or value
  - Unauthorized person can access exactly same digital objects as the original copy
  - Commercially, unauthorized dissemination and use of digital object may cause revenue loss
  - Unauthorized dissemination and use of sensitive information causes information leakage (e.x. intelligence community, health care)

DRM in Nutshell

- It's a system, a technology, a service, an application software, and a solution
- No concrete definition.
  - Many interests groups, many vendors, many solutions, but no standards
  - Little interoperability
- Controlling and tracking access to and usage (including dissemination) of digital information objects
- Securing digital object itself, not the transmission
  - By using cryptographic, and watermarking technologies
- Business perspectives
  - Not just for protections, but new business models
  - Increased revenue

Variations of DRM definition

- Originally,
  - to capture a set of new technologies that enables controlling use of digital contents after the contents are distributed to clients.
- Today,
  - vary by different researchers and scientists
  - unclear what should be included in DRM boundary and what DRM is capable of.

DRM Definition - Rosenblatt et al. 2002

- In their book, Rosenblatt et al. refers DRM as controlling and managing legal, transactional, and implicit rights to digital intellectual property.
  - **Legal:** Rights that you get either automatically under law (such as inherent copyright) or by some legal procedure (such as applying for a patent)
  - **Transactional:** Rights that you get or give up by buying or selling them, such as buying a book or selling a manuscript to a publisher
  - **Implicit:** Rights defined by the medium that the information is in

DRM Definition – Robson 2003

- In his article "The TEACH Act and The MPEG Rights Expression Language", Robson defines
  - DRM is a technology that restricts or prevents the unauthorized use of digital contents in accordance with defined rights and conditions.
  - DRM is the process of defining, tracking and enforcing permissions and conditions through electronic means.

DRM Definition – Iannella 2001

- In "DRM architectures", d-lib, Iannella tries to capture the evolution of DRM definitions by saying that
  - DRM focused on security and encryption as a means of solving the issue of unauthorized copying, that is, lock the content and limit its distribution to only those who pay. This was the first-generation of DRM.
  - The second-generation of DRM covers the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders relationships.

DRM Definition –various scopes

- Rosenblatt tries to include more than technologies within DRM scope (such as business and legal issues)
- Robson tries to include only technological issues (specifically, emphasizing both protections and tracking) within DRM definition.
- Iannella tries to capture wide range technologies

DRM Definition - Ambiguity

- many researchers and scientists tried to define the meaning and scope of DRM
- Still ambiguous in its definition, scope, and meaning.
- The references in previous slides show that there is no airtight, single definition of DRM.
- DRM technologies vs. DRM applications

Basic functions of a DRM system

- Basic functions:
  - Systems that content providers can use internally for defining, organizing, and managing contents and rights
  - Systems for distributing content to consumers in a controlled way
  - Systems for managing usage to content
  - Systems for licensing and distributing content to other publishers in a controlled way
  - Systems for measuring content usage
  - Payment systems
  - …
- Functions can be integrated or separated.

Understanding DRM

- Some of DRM aspects
  - Dissemination Scale
    - Small, medium, and large scale
  - Dissemination Environment
    - Closed, federated, open, and p2p environment
  - Payment-based vs. Payment-free
  - Prevention vs. Detection & Tracking

Dissemination Scale

- Small Scale Dissemination
  - 1 item → 1 to 100 recipients
  - Much less tolerance for leakage
  - B2B Business transaction, Intelligence community
- Medium Scale Dissemination
  - 1 item → 10^3 to 10^5 recipients
  - Textbook publishing, technical journals
- Large Scale Dissemination
  - 1 item → 10^6 to 10^8 recipients
  - Some leakage is acceptable or even desirable
  - Music, popular books

Dissemination Environment

- Closed Environment Dissemination
  - Internal distribution (commercial and Intelligence)
  - Easy to customize client-side systems (both S/W & H/W)
- Federated Environment Dissemination
  - Limited number of organizations are involved
  - B2B, B2G and G2G dissemination
  - Limited administrative control over recipients
- Open Environment Dissemination
  - B2B and B2C dissemination
  - Hard to customize client-side system
- P2P Environment Dissemination

Two Types of Dissemination

- Payment-Based Type (PBT)
  - Payment is required in order to access digital content
  - B2C mass distribution e-commerce system
- Payment-Free Type (PFT)
  - Payment is not required
  - Dissemination must be controlled for confidentiality or other security requirements
  - B2B Hub System, G2G, Intelligence Community

Characteristics of PBT & PFT

- Payment-Based
  - A small amount of information leakage is acceptable and even desired
  - The number of legitimate copies of a single digital item is usually greater than that of PFT
  - The objective in PBT is to distribute as many copies as possible and extract payment
- Payment-Free
  - Information leakage is not acceptable
  - The number of legitimate copies of a single digital item is less than that of PBT
  - It is the distribution itself which needs to be limited
  - The security requirements are likely to be more stringent than that of PBT

Prevention vs. Detection

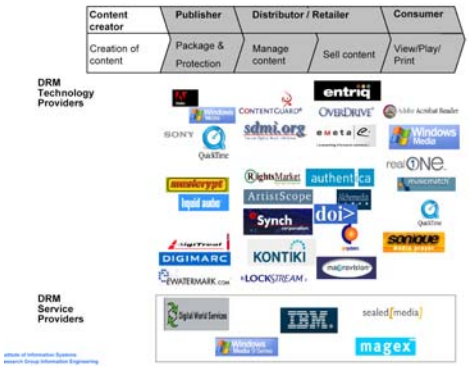
- Prevention
  - Leakage "cannot" occur
- Detection & Tracking
  - Leakage can occur but can be detected and tracked to re-distributor
- Both solutions can/must coexist

Commercial Interest

	Payment	Scale	Environment	Prevent vs. Detect
Major Commercial Interest	Yes	Large Medium	Open Federated Closed	Both
Less Commercial Interest	No	Medium Small	Open Federated Closed	Both (Prevention emphasis)

DRM systems overview

- Heterogonous requirements
- Many techniques
- Huge number of providers



Comparing the Usage of **Digital Rights**. **Management Systems in the** Music, Film, and Print, Fetscherin & Schmid, 2003

DRM Overview

- Objectives:
  - Mainly for technical objectives
- Models:
  - access control or usage control model
- Architectures:
  - Distribution architectures
  - Enforcement architectures
  - Other supported architectures
- Mechanisms:
  - Mechanisms to control the distribution/dissemination
  - Mechanisms to control the usage
  - Payment mechanisms

DRM objectives

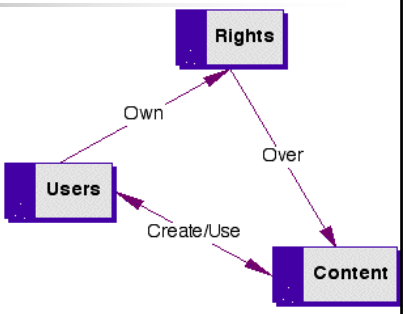
- Mainly for protection of intellectual property rights and copyrights
- Also detection and tracking of (unauthorized) usage
- Controlling and tracking usage of digital objects even after distribution
- Originator control in non-closed environment
- Broader scope includes
  - business, legal, social issues, etc.
  - Content creation, management, re-distribution, etc

Access Control in DRM

- Payment based access control
  - Authorization is based on payment
  - Most of commercial solutions
- Non-payment based access control
  - Little studies on this for DRM
  - MAC, DAC, RBAC, ORCON
  - Non-commercial (e.g., intelligence community, health care)
- UCON can be used as model for DRM systems
- ORCON can be viewed as the core policy for many DRM systems.
  - UCON can support ORCON policy

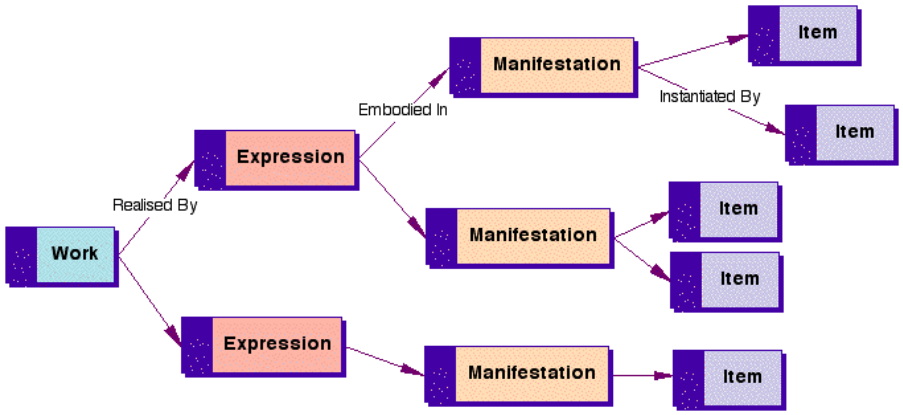
Access Control Model in DRM

- Entity Model(by Iannella)
  - Users:
    - owner, distributor, consumer
  - Objects: digital assets with values
    - Security sensitive
    - Privacy sensitive
  - Rights: usage permissions
    - need to be modeled
  - Each entity should be identified and described with metadata.
    - User attributes
    - Object identifies
    - Rights descriptions



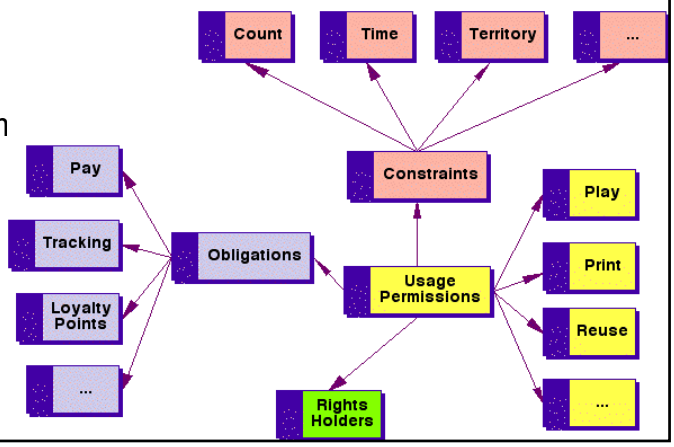
Access control Model in DRM

- Content model: (by Iannella)



Access Control Model in DRM

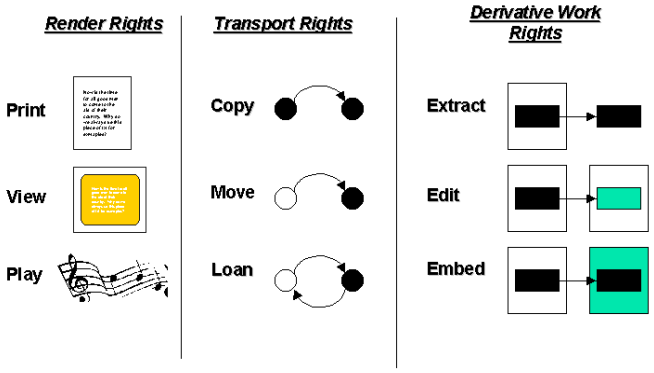
- Right Model (by Iannella)
- DRM is generally closed system



Usage Rights in DRM by Stefik

- Render Rights
  - View, play, print
- Transport Rights
  - Copy, move, loan
- Derivative Work Rights
  - Extract, edit, embed
- File management rights (backup, restore, etc.)
- Configuration rights (install, uninstall)

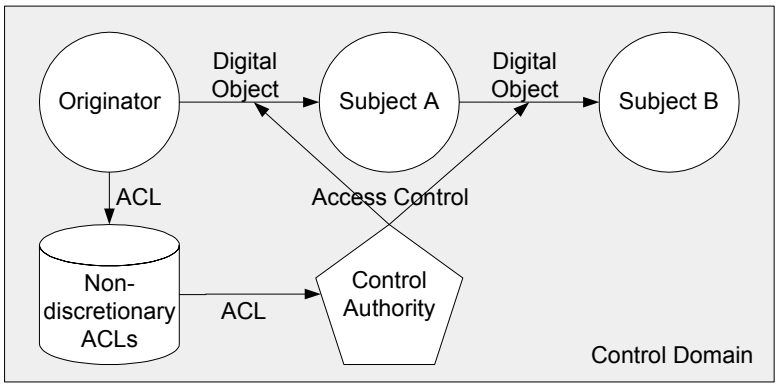
Usage Rights



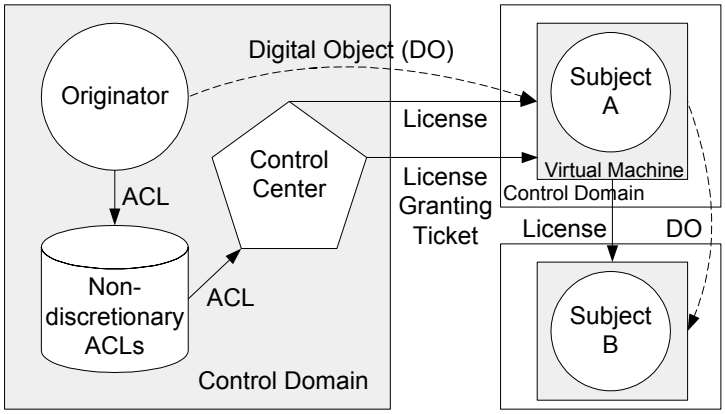
Usage controls in DRM

- Mainly payment-based (can be viewed as authorization or obligation)
  - Paid download, pay-per-view/listen, subscription, metered payment
- Payment-free is possible
  - Authorization-based (ID, role, membership-based)
  - Obligation-based (e.g., parental control, by providing personal info, license agreement)
  - condition-based (e.g., location, time, security status (normal, high-alert), system load, etc.

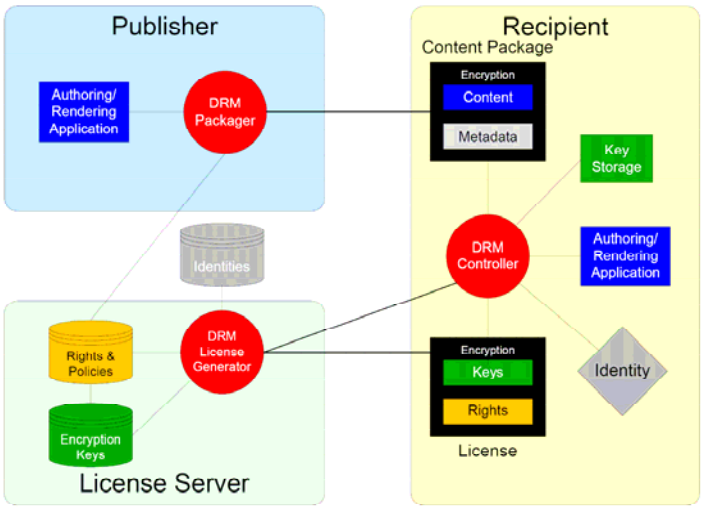
Traditional Originator Control (ORCON)



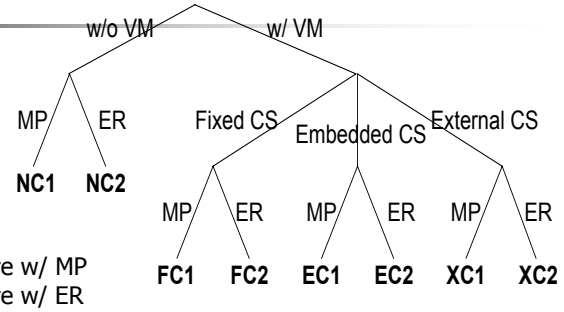
ORCON in Open Environment - An Example



DRM Architecture by Rosenblatt et al.



DRM Architectures by Park et al.



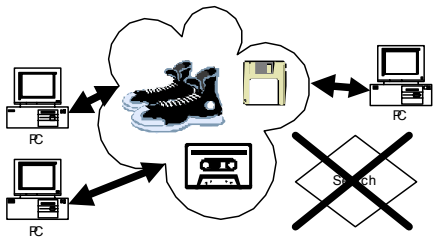
VM: Virtual Machine
CS: Control Set
MP: Message Push
ER: External Repository

NC1: No control architecture w/ MP
NC2: No control architecture w/ ER
FC1: Fixed control architecture w/ MP
FC2: Fixed control architecture w/ ER
EC1: Embedded control architecture w/ MP
EC2: Embedded control architecture w/ ER
XC1: External control architecture w/ MP
XC2: External control architecture w/ ER

Content Distribution

- Darknet(Biddle et al.):
  - Small-worlds networks

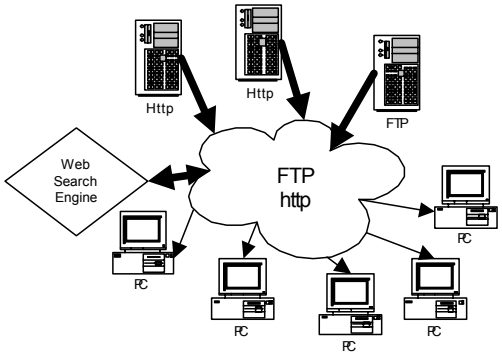
(a) - "Sneaker Net"



Content Distribution

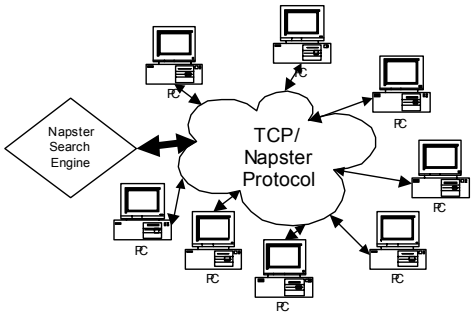
- Central Internet Servers

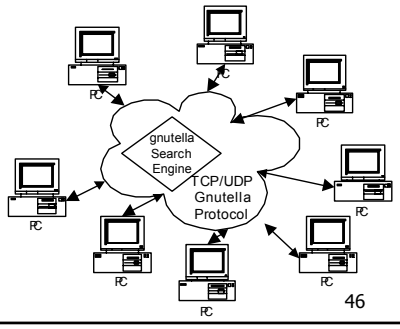
(b) - The World Wide Web



Content Distribution

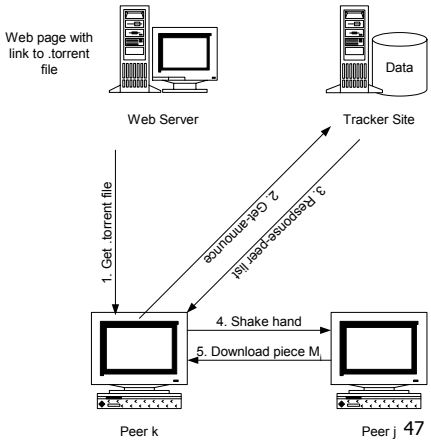
- 1st generation P2P systems
  - Napster, Gnutella
  - DHT



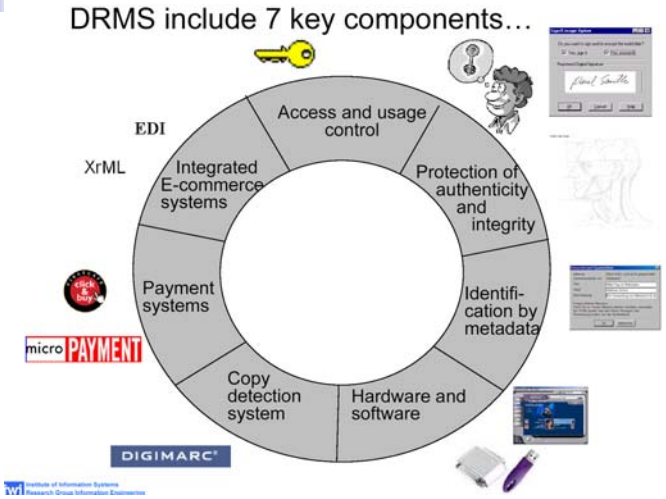


Content Distribution

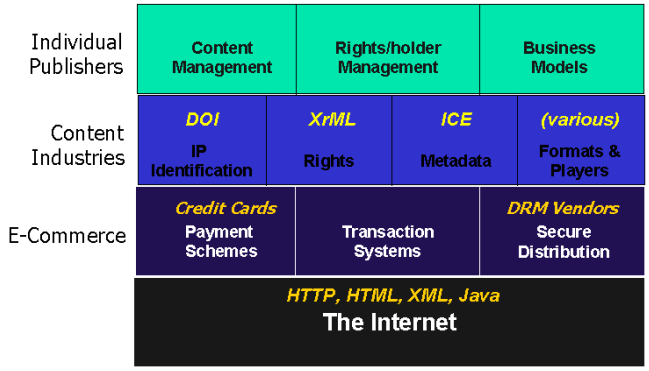
- 2nd P2P systems
  - KaZaA, BitTorrent,



Mechanisms: 7 Key Tech components (Fetscherin & Schmid)



DRM Technology Hierarchy



Digital Watermarking

- Embedding information in information
- Mainly for information authenticity (tracking) and integrity
- Watermarking technologies are dependent on the type of digital information (e.g., text, image, audio and etc.)
- Minimum size of object is required
- Difficulty of embedding different watermark (fingerprint) in each copy of original objects in case of mass distribution

Understanding Digital Watermarking (1)

- Visible Watermarking
  - Watermark is visible (e.g.background logo)
  - Can be used for sample digital objects to reduce commercial value on them
- Invisible Watermarking
  - Most of Watermarking belongs here
  - Digital Watermark can be detected by special software

Understanding Digital Watermarking (2)

- Public Watermarking
  - Watermark information w/ publicly known key (w/o any secret key)
  - Everyone can read watermarked information
  - In commercial sector, customer can find copyright owner's information
- Private Watermarking
  - Only authorized users can detect the watermarks
  - Good for tracking purpose

Understanding Digital Watermarking (3)

- Watermark retrieval
  - Reference-required watermark
    - The original object or embedded watermark information is required for comparison
  - Reference-free watermark
    - Watermark can be retrieved without the original document or added information
    - The mechanism detects specific properties and patterns from documents

Understanding Digital Watermarking (4)

- Different format, different watermarking
  - text, image, audio, and video
- Text Watermarking (Brassil, et al.)
  - Line-shift coding
    - Text lines are shifted imperceptibly up and down
  - Word-shift coding
    - Words are shifted horizontally
    - Original un-watermarked documents are required for extracting watermarked information
  - Feature coding
    - Characters are altered (vertical or horizontal)
    - Least discernible, larger information embedded

Digital watermarking in DRM

- Can be used to embed metadata such as owner's info, usage rights, rules, etc.
- Can provide tracking capability to illicit distribution
- Fingerprinting for individual tracking
- Largely independent from security architectures

Watermarking vs. Encryption in DRM (1) - Rosenblatt et al.

- Both encryption and watermarking can be used to carry metadata for digital contents
  - Using encryption, encapsulate digital contents together with metadata
    - Need special rendering application (CRM)
  - Using watermarking, embed metadata in digital contents
    - No protection on digital contents

Watermarking and Encryption in DRM (2) - Rosenblatt et al.

- Use both for end-to-end secure content distribution
  - Case1: embed metadata, then encrypt watermarked contents
    - Protect both contents and metadata
    - Even after cracking encrypted content, metadata is still bound with the content
  - Case2: encrypt metadata, then embed encrypted metadata into contents
    - temper-resistant, secure watermark
    - Digital timestamping from Surety Inc's digital notary tech., DigiMarc's tracking pirated contents

Commercial Efforts for Open-standard (XrML)

XrML: Extensible Rights Markup Language

- What is XrML?
  - "A language in XML for describing specifications of rights, fees and conditions for using digital contents, together with message integrity and entity authentication within these specifications" (www.xrml.org)
  - An extension of the Xerox "Digital Property Rights Language version 2.0 (DPRL)"
  - ContentGuard™ has developed XrML as an open specification licenced on a royalty-free basis
- Why XrML?
  - In DRM, XrML can be viewed as one of potential mechanisms to express specific rights and rules.
  - XrML is extensible, open specification with license
  - XrML is accepted as a standard for MPEG21

Top-Level Structure

```
<XrML>
    <BODY>
        (TIME)?                    time interval in which this spec is valid
        (ISSUED)?                  time moment at which this spec is issued
        (DESCRIPTOR)?              description or meta data of this spec
        (ISSUER)?                  principal who issues this spec
        (ISSUEDPRINCIPALS)?        list of principals this spec is issued to
          (PRINCIPAL)+
        (WORK)?                    work and rights this spec specifies
        (AUTHENTICATEDDATA)?       data that provided to application
    </BODY>
    (SIGNATURE)?
</XrML>
```

"?" denotes zero or one occurrence; "+" denotes one or more occurrences; and "*" denotes zero or more occurrences

Digital Works & Usage Rights

```
<WORK>
    OBJECT          object used to identify the work
    DESCRIPTION     description of the work
    CREATOR         creator of the work
    OWNER           owner of the work
    METADATA        additional metadata of the work
    DIGEST          digest value of the work
    PARTS           parts of the work, each of which is a work itself
    CONTENTS        indicator of where content of the work is
    COPIES          number of copies of the work that are specified
    COMMENT         Comment
    SKU             Stock Keeping Unit, for extensibility to allow people to
                    identify this work in their own stock.
    FORMAT          Digital or physical manifestation of the work
    (RIGHTSGROUP | REFERENCEDRIGHTSGROUP )+   rights group associated
                    with the work | reference rights group of the work
</WORK>
```

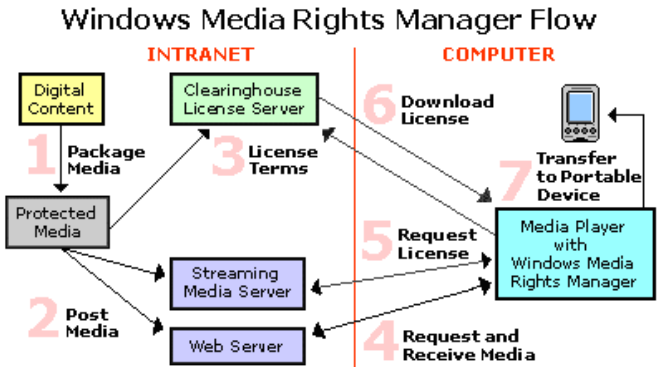
Rights in RIGHTSGROUP Element

- Digital property rights
- Specifying times, fees and incentives
- Specifying access controls (licenses/certificates, security levels)
- Specifying territory information
- Specifying tracking information
- Specifying watermark information
- Bundle specifications (time limits, fees, access, and watermark info inside bundle)

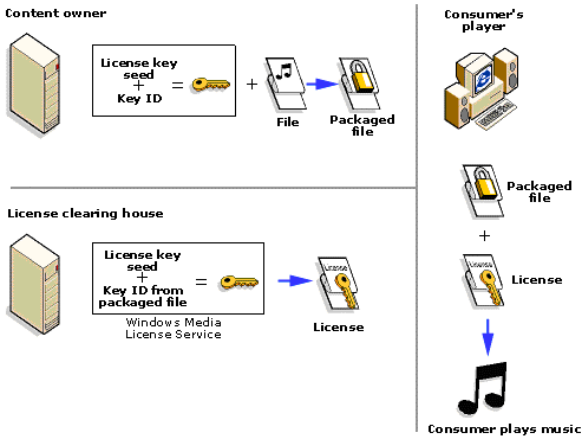
Case Study

Windows Media Digital Rights Management

Workflow



Encryption of content



License

- The key to unlock the Windows Media file
- The rights, or rules, that govern the use of the digital media file:
  - How many times can a file be played
  - Which devices a file can be played or transferred on.
  - When the user can start playing the file and what is the expiration date.
  - If the file can be transferred to a CD recorder (burner).
  - If the user can back up and restore the license.
  - What security level is required on the client to play the Windows Media file.
  - …

Related Issues

Fair Use

- Fair use provides an exemption on legal liability for the use of copyrighted materials.
  - To limit copyright owner's exclusive rights on copyrighted materials
  - Reproduction or other means for criticism, news reporting, teaching, scholarship, and research is fair use and not an infringement of copyrights [section 107]

First Sale

- When you buy a physical book, you can do anything you want on your copy and your copy only.
  - Read, sell, destroy, give away, etc.
  - You buy a copy, you own the copy.
- However, no rights on copyrights

Purchase vs. License

- In general, digital contents are not sold but licensed
- When you are licensing, you don't buy anything but a right to use (read, listen, run, etc.) the copy
- By agreeing on a license, you may give up your rights for fair use and first sale.
- License is contract law and shouldn't be overridden federal copyrights law.

Fair use and first sale in DRM

- DRM largely relies on licensing
- There exists a great fear about DRM because license agreement can give away rights on fair use and first sale
- Fair use is very difficult or impossible to implement in DRM because it cannot be pre-judged
- First sale is not likely to be allowed in licensing (e.g., MS windows OS)

Digital Millennium Copyright Act (DMCA)

- Legislated in 1998
- "anti-circumvention provision", in Section 1201 is most controversial.
  - Implies that copy protection technology is not perfect
  - Abused to override copyright law such as fair use